APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,772	02/16/2001	Robert C. Ledzius	QUI200/4-002	2982

7590	12/22/2004	

Sally Draper
Quickflex, Inc.
8401 N. New Braunfels,
Suite 324
San Antonio, TX 78209

EXAMINER
NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 12/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/785,772	LEDZIUS ET AL.
	Examiner	**Art Unit**	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>16 February 2001</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-25</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-25</u> is/are rejected.

7)☒ Claim(s) <u>3,6,17</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>2/16/01, 4/30/01, and 7/23/01</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

        1.☐ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-25.

Claim Objections

2.   Claim 3 is objected to under 37 CFR 1.75(c), as being of improper dependent

form for failing to further limit the subject matter of a previous claim. Applicant is

required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper

dependent form, or rewrite the claim(s) in independent form. Claim 3 provides the

limitation "transmitting said encrypted session key to said data server." Claim 3

depends from claim 2 and provides the same limitation in lines 23-24.

3.   Claim 6 is objected to because of the following informalities: Applicant has

provided two claims numbered as claim 6. The first of such claims, claim 6 depending

from claim 1 and providing the limitation "decrypting said set of encrypted data using

said second private key at said client," has been interpreted to be a typo for the

remainder of this office action and will hereafter be referred to as claim 25. The

remaining claim 6, an independent claim, will continue to be referenced as currently

presented. Appropriate correction is required.

4.   Claim 17 is objected to because of the following informalities: Claim 17 contains

the typo "sever" on line 7.

Drawings

5.   This application has been filed with informal drawings which are acceptable for

examination purposes only. Formal drawings will be required when the application is

allowed.

Claim Rejections - 35 USC § 112

6.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

7.   Claim 14 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention. The term " substantially " in claim 14 is a relative term which

renders the claim indefinite. The term "substantially" is not defined by the claim, the

specification does not provide a standard for ascertaining the requisite degree, and one

of ordinary skill in the art would not be reasonably apprised of the scope of the

invention.

8.   Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention. The cited claim provides the limitation "wherein said first

private cipher is not stored in memory." This limitation is unclear because in computing

systems all data must at some point be stored in memory.

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

10.   Claims 1, 6-18, 20, 22, and 24 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ganeson US Patent No. 5,557,678 in view of Sachs et al US Patent

No. 6,331,865. Ganeson discloses a system for centralized session key distribution.

Sachs discloses a method for electronically distributing and viewing digital contents.

11.   With regards to claims 1, Ganeson teaches the storing of a first set of data on a

data server with the first set of data being encrypted by a first private key (Ganeson,

column 10 lines 42-46, encrypted video), establishing a set of rules for responding to a

data request from the client and storing the rules on the data server (Ganeson, column

7 lines 4-7), generating a first private key at the security server with the first private key

associated with the data server (Ganeson, column 8 lines 27-35, column 9 lines 1-3,

private portion for station 30), generating a second private key at the security server

with the second private key associated with the client (Ganeson, column 8 lines 27-35,

column 9 lines 1-3, private portion for station 32), and the generating of a session key at

the security server (Ganeson, column 10 lines 52-53, station 50). Ganeson fails to

teach the transmitting of an authentication request from the data server to the security

server and authenticating the user responsive to the authentication request. Sachs

teaches the transmitting of an authentication request from the data server to the security

server (Sachs, column 3 lines 54-63, authentication server called upon) and the

authenticating the user responsive to the authentication request (Sachs, column 3 lines

54-57, client authentication). At the time the invention was made, it would have been

obvious to a person of ordinary skill in the art to utilize Sachs' authentication method

with Ganeson's key distribution system because it offers the advantage of allowing

identification of a client so as to ensure that data is only readable by an authorized client

(Sachs, column 1 lines 36-55).

12.   With regards to claims 6, 13, and 14 (as best understood), Ganeson teaches a

data server having an encryption/decryption engine (Ganeson, column 10 lines 42-46,

video distributor) and a first private cipher (Ganeson, column 10 lines 58-62, private

portion of encryption key), a user device in electrical communication with the data

server for sending data request and receiving a set of responsive data (Ganeson,

column 10 lines 50-52, station 38, column 11 line 3), the user device having a second

private cipher (Ganeson, column 10 lines 58-62), and a security server having a third

private cipher (Ganeson, column 10 lines 52-53, session key) in communication with the

user device and the data server and wherein the security server established a secure

transmission link (Ganeson, column 11 lines 19-22). Ganeson fails to teach the data

server being configured to respond to a data request from a user device. Sachs

teaches the data server is configured to respond to a data request from a user device

(Sachs, column 3 lines 54-58, electronic book requests data from bookstore). At the

time the invention was made, it would have been obvious to a person of ordinary skill in

the art to utilize Sachs' method of requesting data because it offers the advantage of

providing a distinct catalog of digital works available to the client (Sachs, column 1 lines 36-62).

13.   With regards to claims 11-12, Ganeson as modified teaches the third private cipher being randomly generated (Sachs, column 3 line 60, unique session key).

14.   With regards to claim 15 (as best understood), Ganeson as modified teaches the first private cipher not stored in memory (Ganeson, column 8 lines 51-57, other manner).

15.   With regards to claim 16 (as best understood), Ganeson as modified teaches the first private cipher not accessible on any bus (Ganeson, column 8 lines 51-57, other manner).

16.   With regards to claim 17, Ganeson teaches the generating of the session key at the security server (Ganeson, column 8 lines 63-64, session key), the generating of a first secret key for the data server (Ganeson, column 8 lines 27-35, column 9 lines 1-3, private portion for station 30), generating a second secret key for the user device (Ganeson, column 8 lines 27-35, column 9 lines 1-3, private portion for station 32), transmitting data from the data server to the user device via the secure data transmission session (Ganeson, column 11 lines 19-22), the encrypting of the random session key with the first secret key resulting in a first encrypted random session key and transmitting the first encrypted session key to the server (Ganeson, column 8 line 67 – column 9 line 6, key for station 30), and the encrypting of the random session key with the second secret key resulting in a second encrypted random session key and transmitting the second encrypted random session key (Ganeson, column 8 line 67 –

column 9 line 10, key for station 32). Ganeson fails to teach the validating of a data

server and a user device requesting the secure data transmission session. Sachs

teaches the validating of a data server and a user device requesting the secure data

transmission session (Sachs, column 3 lines 64-62, and column 4 lines 1-3). At the

time the invention was made, it would have been obvious to a person of ordinary skill in

the art to utilize Sachs' authentication method with Ganeson's key distribution system

because it offers the advantage of allowing identification of a client so as to ensure that

data is only readable by an authorized client (Sachs, column 1 lines 36-55).

17.   Claims 7-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Ganeson US Patent No. 5,557,678 and Sachs et al US Patent No. 6,331,865, as

applied to claim 6 above, in further view of Challener et al US Patent No. 6,718,468.

18.   With regards to claim 7, Ganeson as modified fails to teach the data server

comprising a PCI board for hosting the encryption/decryption engine. Challener

teaches the use of a PCI board for hosting the encryption/decryption engine (Challener,

column 3 lines 41-43). At the time the invention was made, it would have been obvious

to a person of ordinary skill in the art to utilize Challener's method of using PCI boards

to host encryption engines with Ganeson as modified because it offers the advantage of

providing a low latency and high bandwidth data path for communication between the

processor and PCI devices (Challener, column 3 lines 18-27).

19.   With regards to claims 8 and 10, Ganeson as modified teaches an erasable

memory for storing the second encryption key (Challener, column 3 lines 40-54,

protected storage area). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Challener's method of storing keys with Ganeson as modified because it offers the advantage of providing a protected storage area for encryption keys that is not assessable to any other computing component (Challener, column 3 lines 50-52).

20.   With regards to claim 9, Ganeson as modified teaches the use of erasable memory, as described above, but fails to specifically teach the use of flash memory. Examiner hereby takes official notice that the use of flash memory is well known in the art and thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use flash memory as a form of erasable memory with Ganeson as modified because it offers the advantage of providing a fast and easy method of storing information that is solid state and thus requires no moving parts.

21.   With regards to claim 18, Ganeson as modified teaches the session key being hardware generated (Ganeson, column 8 lines 63-64, processor generated).

22.   With regards to claims 20 and 22, Ganeson as modified teaches the first and second secret keys being hardware generated (Ganeson, column 8 lines 26-35, processor generates first private key portion for each user).

23.   With regards to claim 24, Ganeson as modified teaches the decrypting of the data using the random session key, first secret key, and second secret key (Ganeson, column 9 lines 3-22).

24.   Claims 19, 21, and 23 are rejected under 35 U.S.C. 103(a) as being
unpatentable over Ganeson US Patent No. 5,557,678 and Sachs et al US Patent No.
6,331,865, as applied to claim 17 above, in further view of Yin US Patent No. 6,028,939.
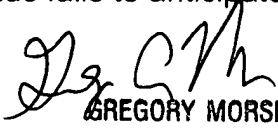
25.   With regards to claim s 19, 21, and 23, Ganeson as modified fails to teach the
hardware generating the random session key being reconfigurable. Yin teaches
encryption hardware that is reconfigurable (Yin, column 7 line 30 column 8 line 38,
programmable hardware element). At the time the invention was made, it would have
been obvious to a person of ordinary skill in the art to utilize Yin's method of allowing
reconfiguration with Ganeson as modified because it offers the advantage of providing
flexibility to incorporate new or different algorithms and processes for encryption (Yin,
column 2 lines 37-43).

Allowable Subject Matter

26.   Claims 2-5 and 25 are objected to as being dependent upon a rejected base
claim, but would be allowable if rewritten in independent form including all of the
limitations of the base claim and any intervening claims.

27.   The following is a statement of reasons for the indication of allowable subject
matter: Claim 2 provides the limitations of, "transmitting said first encrypted session key
and said second encrypted session key to said data server; and transmitting said
second encrypted session key to said client." The cited prior art fails to specifically
teach or suggest the all of the limitations of claim 2 and thus fails to anticipated or
render obvious the above cited claims.

* See objection to Cl. 6. *Dm*

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conclusion

28.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

29.   Torii et al US Patent No. 5,313,521 discloses a key distribution protocol for file

transfer in a local area network.

30.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Andrew L Nalven whose telephone number is 571 272

3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate

Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven